

(43)Date of publication of application : 10.12.1999

H04M 11/00

(72)Inventor : ISHIKAWA YOSHIHARU

Serial	Number	Year	Model	Manufacturer	Ref
012524	000001	1974	012524	012524	012524
012525	000002	1974	012525	012525	012525
012526	000003	1974	012526	012526	012526
012527	000004	1974	012527	012527	012527
012528	000005	1974	012528	012528	012528
012529	000006	1974	012529	012529	012529
012530	000007	1974	012530	012530	012530
012531	000008	1974	012531	012531	012531
012532	000009	1974	012532	012532	012532
012533	000010	1974	012533	012533	012533
012534	000011	1974	012534	012534	012534
012535	000012	1974	012535	012535	012535
012536	000013	1974	012536	012536	012536
012537	000014	1974	012537	012537	012537
012538	000015	1974	012538	012538	012538
012539	000016	1974	012539	012539	012539
012540	000017	1974	012540	012540	012540
012541	000018	1974	012541	012541	012541
012542	000019	1974	012542	012542	012542
012543	000020	1974	012543	012543	012543
012544	000021	1974	012544	012544	012544
012545	000022	1974	012545	012545	012545
012546	000023	1974	012546	012546	012546
012547	000024	1974	012547	012547	012547
012548	000025	1974	012548	012548	012548
012549	000026	1974	012549	012549	012549
012550	000027	1974	012550	012550	012550
012551	000028	1974	012551	012551	012551
012552	000029	1974	012552	012552	012552
012553	000030	1974	012553	012553	012553
012554	000031	1974	012554	012554	012554
012555	000032	1974	012555	012555	012555
012556	000033	1974	012556	012556	012556
012557	000034	1974	012557	012557	012557
012558	000035	1974	012558	012558	012558
012559	000036	1974	012559	012559	012559
012560	000037	1974	012560	012560	012560
012561	000038	1974	012561	012561	012561
012562	000039	1974	012562	012562	012562
012563	000040	1974	012563	012563	012563
012564	000041	1974	012564	012564	012564
012565	000042	1974	012565	012565	012565
012566	000043	1974	012566	012566	012566
012567	000044	1974	012567	012567	012567
012568	000045	1974	012568	012568	012568
012569	000046	1974	012569	012569	012569
012570	000047	1974	012570	012570	012570
012571	000048	1974	012571	012571	012571
012572	000049	1974	012572	012572	012572
012573	000050	1974	012573	012573	012573
012574	000051	1974	012574	012574	012574
012575	000052	1974	012575	012575	012575
012576	000053				

2001/07/09 17:20

(11)特許出願公開番号

特開平11-341151

(43)公開日 平成11年(1999)12月10日

(51) Int.Cl.⁶

識別記号

FI

H O 4 M 1/66

H O 4 M 1/66

C

G O 6 F 15/00

3 1 0

G O 6 F 15/00

3 1 0 C

H0 4M 11/00

3 0 3

H0 4M 11/00

3 0 3

審査請求 有 請求項の数 3 O L (全 6 頁)

(21)出願番号

特願平10-150114

(22) 出願日

平成10年(1998)5月29日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 石川 義晴

東京都港区芝五丁目7番1号 日本電気株
式会社内

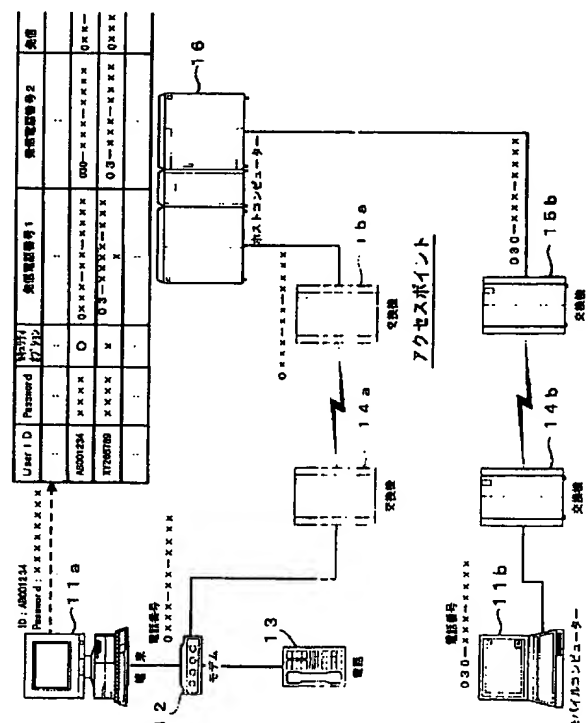
(74)代理人 弁理士 高橋 詔男 (外3名)

(54) 【発明の名称】 ダイヤルアップ接続認証方式

(57) 【要約】

【課題】 ダイヤルアップによるインターネット接続やパソコン通信サービスにおいて、より確実なアカウントの確認を行う。

【解決手段】 ユーザ側端末１１aは、サービス提供者側のアクセスポイントに対してダイヤリングを行う。このとき、発信電話番号がホストコンピュータ１６へ通知される。また、回線が接続されると、ユーザIDとパスワードがホストコンピュータ１６へ送信される。ホストコンピュータ１６では、通常の接続時と同様にユーザID、パスワードの確認を行った後、そのままサービス提供を開始せずに、さらに、発信電話番号をチェックし、一致すれば、接続を認証して各種サービス提供を開始する。



【特許請求の範囲】

【請求項 1】 ダイヤルアップにより接続要求してきた端末に対してユーザ認証を行うダイヤルアップ接続認証方式において、

予め、ユーザ毎の発信電話番号を記憶しておき、前記端末から接続要求があると、着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致するか否かを判断することでユーザ認証を行うことを特徴とするダイヤルアップ接続認証方式。

【請求項 2】 前記ユーザ認証の前後に、回線接続後に端末から送信されるユーザ ID およびパスワードと予め登録されているユーザ ID およびパスワードとを比較し、それぞれ双方が一致するか否かを判断することで第 2 のユーザ認証を行うことを特徴とする請求項 1 記載のダイヤルアップ接続認証方式。

【請求項 3】 着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致した場合、少なくとも予め記憶していた発信電話番号を含むユーザ情報の更新を許可することを特徴とする請求項 1 記載のダイヤルアップ接続認証方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ダイヤルアップによるインターネット接続やパソコン通信サービスにおいて、サービス提供者／プロバイダが回線接続時にサービス利用者のアカウントを確認するためのダイヤルアップ接続認証方式に関する。

【0002】

【従来の技術】ダイヤルアップによるインターネット接続やパソコン通信サービスにおいては、ユーザ端末側からサービス提供者側のアクセスポイントに対し、ダイヤリングを行い、サービス提供者側は、ユーザ端末側から送信されるユーザ ID 及びパスワードにより、そのユーザ認証を行ってサービス提供を開始する。

【0003】

【発明が解決しようとする課題】しかしながら、従来技術では、第三者にユーザ ID とパスワードが漏洩し、不正に利用された場合、サービス提供者はサービス利用時間や特定のサービス利用の内容に応じて、ユーザ ID を持つ利用者に対して利用料として課金を行うため、ユーザ ID の不正利用により、正規ユーザが多大な損害を受けてしまうという問題があった。

【0004】この発明は上述した事情に鑑みてなされたもので、ダイヤルアップによるインターネット接続やパソコン通信サービスにおいて、サービス提供者／プロバイダが回線接続時にサービス利用者のアカウントを確認する際に発信電話番号通知情報を利用して、より確実なアカウントの確認を行うことができるダイヤルアップ接続認証方式を提供することを目的とする。

【0005】

【課題を解決するための手段】上述した問題点を解決するために、請求項 1 記載の発明では、ダイヤルアップにより接続要求してきた端末に対してユーザ認証を行うダイヤルアップ接続認証方式において、予め、ユーザ毎の発信電話番号を記憶しておき、前記端末から接続要求があると、着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致するか否かを判断することでユーザ認証を行うことを特徴とする。

【0006】また、請求項 2 記載の発明では、請求項 1 記載のダイヤルアップ接続認証方式において、前記ユーザ認証の前後に、回線接続後に端末から送信されるユーザ ID およびパスワードと予め登録されているユーザ ID およびパスワードとを比較し、それぞれ双方が一致するか否かを判断することで第 2 のユーザ認証を行うことを特徴とする。

【0007】また、請求項 3 記載の発明では、請求項 1 記載のダイヤルアップ接続認証方式において、着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致した場合、少なくとも、予め記憶していた発信電話番号を含むユーザ情報の更新を許可することを特徴とする。

【0008】この発明では、サービス利用者からの着信の度に発信電話番号と登録済みの発信電話番号とを照合する。したがって、第三者によるアカウントの不正利用を防止することが可能となる。

【0009】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

A. 実施形態の構成

図 1 は、本発明の実施形態による全体の構成を示すブロック図である。図において、端末 11 a は、ユーザ側の固定端末であり、モデム 12 により発信し、交換機 14 a を介して電話網に随時接続する。モデム 12 には、通常の電話機も接続することが可能である。この場合、端末 11 a からのホストコンピュータ 16 への発信は、常時、同じ発信電話番号となる。交換機 14 a は、図示の例では発信側の交換機であり、電話網に接続され、モデム 12 による発信に従って、着信側の交換機 15 a に接続する。また、交換機 15 a は、図示の例では着信側（サービス提供者側）の交換機であり、電話網に接続され、交換機 14 a からの着信を受け付け、ホストコンピュータ 16 に接続する。

【0010】また、端末（モバイルコンピュータ）11 b は、ユーザ側の移動端末であり、その位置に応じた交換機 14 b を介して電話網に随時接続する。この場合、端末 11 b からのホストコンピュータ 16 への発信は、その都度、異なる発信電話番号となる可能性がある。交換機 14 b は、図示の例では発信側の交換機であり、電

話網に接続され、モバイルコンピュータ 1 1 b からの発信に従って、着信側の交換機 1 5 b に接続する。また、交換機 1 5 b は、図示の例では着信側（サービス提供者側）の交換機であり、電話網に接続され、交換機 1 4 b からの着信を受け付け、ホストコンピュータ 1 6 に接続する。

【0 0 1 1】サービス提供者側のホストコンピュータ 1 6 は、ユーザ認証を行うために、ユーザ ID、パスワード、セキュリティオプションフラグ、複数の発信電話番号、を対応付けてユーザプロファイル情報として記憶している。ホストコンピュータ 1 6 は、着信側交換機 1 5 a、1 5 b から通知される発信電話番号と登録済みの発信電話番号との比較を行う。発信電話番号は、1 9 9 8 年 2 月より全国的に開始されている、着信者側に発信者側の電話番号を通知するサービスにより、交換機 1 4 a、1 5 a（または 1 4 b、1 5 b）を介して着信者側に通知される。なお、ホストコンピュータ 1 6 に記憶されているユーザ認証用のユーザプロファイル情報の詳細については後述する。

【0 0 1 2】次に、図 2 は、図 1 に示すサービス提供者側のアクセスポイント及びホストコンピュータの詳細な構成が示すブロック図である。図 2 において、中継装置 2 2 は、電話網 2 1 から着信を受け付け、それとともに発信電話番号の通知を受ける。通知された発信電話番号を発信電話番号記憶部 2 3 へ退避するとともに専用線等の回線を通じ、ホストコンピュータ 1 6 との通信を開始する。また、ユーザ端末側 1 1 a とサービス提供者側のホストコンピュータ 1 6 とのユーザ ID、パスワードの認証確認後、発信電話番号記憶部 2 3 に退避した発信電話番号をホストコンピュータ 1 6 へ送信する。

【0 0 1 3】サービスマネージャ 2 4 は、ユーザ端末 1 1 a 側から送信されるユーザ ID を受信し、ホストコンピュータ 1 6 上に記録されているユーザプロファイル情報 2 6 を参照する。続けて、ユーザ端末側からはユーザ固有のパスワードが送信されるので、受信したパスワードとユーザプロファイル情報 2 6 に記録されている情報が一致することを確認する。ここでの情報の不一致が生じた場合には、ユーザ端末 1 1 a 側に対し、パスワードの再入力等を要求する等の復旧手段を講ずる必要があるが、本発明の適用範囲外であるためその詳細についての説明は省略する。

【0 0 1 4】パスワードによる認証確認後、アクセスポイントの中継装置 2 2 から発信電話番号記憶部 2 3 に退避されている発信電話番号を受信し、発信電話番号管理部 2 5 へ退避するとともにユーザプロファイル情報 2 6 に定義されている 1 つ以上の登録発信電話番号および発信電話番号の確認（発信電話番号確認機能）を行うか否かを明示するフラグ（セキュリティオプションフラグ）を参照し、その設定内容に応じて、追加のユーザ認証を行う。ここでセキュリティオプションフラグ及び 1 つ目

の登録発信電話番号（第一登録発信電話番号）のデフォルト値は、各々、発信電話番号の確認を行わない設定、サービス利用申請時の登録電話番号となっている。

【0 0 1 5】利用者が発信電話番号確認機能を利用するためには、ユーザプロファイル情報 2 6 に定義される第一登録発信電話番号の回線からユーザ端末 1 1 a 側が通信サービスを利用し、これらの情報を変更する。ユーザ端末 1 1 a 側から、これらのセキュリティ情報の変更が要求されると、発信電話番号管理部 2 5 に退避してある発信電話番号とユーザプロファイル情報 2 6 に含まれる第一登録発信電話番号とを比較し、一致した場合に限り、ユーザプロファイル情報 2 6 に含まれる、これらのセキュリティ情報の更新を可能とする。利用者は、複数の登録発信電話番号を登録しておくことにより、携帯電話等を使用したモバイルコンピュータ 1 1 b により、外出先から通信サービスを利用することが可能となる。

【0 0 1 6】B. 実施例の動作

次に、図 3 に示すフローチャートを参照して本実施例の全体の動作について詳細に説明する。まず、図 1 のユーザ側端末 1 1 a から、サービス提供者側のアクセスポイントに対してダイヤリングを行う。サービス提供者側は、アクセスポイントの中継装置 2 2 において、電話網 2 1 から着信を受けるとともに発信電話番号の通知を受けることが可能である。中継装置 2 2 は、専用線等の回線を通じて、ホストコンピュータ 1 6 と通信を開始するとともに、発信電話番号記憶部 2 3 に着信時に通知された発信電話番号を記憶する（ステップ S 3 1）。

【0 0 1 7】ホストコンピュータ 1 6 側で一連のサービス提供を制御するサービスマネージャ 2 4 では、通常の接続時と同様にユーザ ID の確認を行い（ステップ S 3 2）、ユーザプロファイルデータ情報 2 6 を参照し、パスワード確認を行う（ステップ S 3 3）。パスワード確認後、そのままサービス提供を開始せずに、さらに発信電話番号の確認を行う（ステップ S 3 4）。該発信電話番号確認処理について以下に詳細に説明する。

【0 0 1 8】次に、図 4 は、図 3 の発信電話番号確認処理（ステップ S 3 4）の詳細な動作を説明するためのフローチャートである。まず、アクセスポイントの中継装置 2 2 からステップ S 3 1 で発信電話番号記憶部 2 3 に退避していた発信電話番号を受信し、発信電話番号管理部 2 5 へ退避するとともに、ステップ S 3 2 で取得済みのユーザ ID に対応するユーザプロファイルデータ情報 2 6 から発信電話番号確認を行うための情報（発信電話番号情報）を取得する（ステップ S 4 1）。

【0 0 1 9】次に、ステップ S 4 1 で取得した発信電話番号情報の 1 つである発信電話番号確認サービスの利用の有無を判別するためのフラグを参照し、本サービスを利用しない設定に定義してある場合には、そのまま接続を認証し、各種サービス提供を開始する（ステップ S 4 2）。一方、本サービスを利用する設定にしてある場合

には、ユーザプロフィール情報 2 6 に設定されている発信電話番号情報をチェックし（ステップ S 4 3、ステップ S 4 4）、一致するものがあれば、接続を認証し、各種サービスプログラム 2 7 によるサービス提供を開始する。これに対して、一致するものがなければ、第三者による不正利用と見なし、回線切断処理を行う（ステップ S 4 5）。

【0 0 2 0】次に、図 5 は、サービス提供者側のホストコンピュータ 1 6 上にあるユーザプロフィール情報 2 6 に定義されている発信電話番号情報を更新する際の処理の動作を説明するためのフローチャートである。ユーザプロフィール情報 2 6 に定義されている発信電話番号情報を更新する際には、まず、発信電話番号管理部 2 5 に退避された発信電話番号とユーザプロフィール情報 2 6 に含まれる第一登録電話番号とを比較し（ステップ S 5 1）、これらの情報が一致している場合に限り、セキュリティオプションフラグ及び登録電話番号情報の更新を認める（ステップ S 5 2）。また、発信電話番号が不一致の場合には、ユーザ端末 1 1 a に対して、発信電話番号情報の更新ができない旨、通知を行う（ステップ S 5 3）。

【0 0 2 1】C. 他の実施例

次に、本発明の他の実施例について説明する。上述した実施例においては、発信電話番号が登録済みのデータと一致することを確認し、ユーザ認証を行う方法と登録情報の更新手段とについて説明したが、引越などにより、利用者の電話番号の変更が余儀なくされる場合があり得る。このような場合には、容易に利用環境の移行ができる必要がある。

【0 0 2 2】そこで、通常利用する登録発信電話番号とは別に移行予定の発信電話番号（予約発信電話番号）を登録しておき、発信電話番号確認手順のステップ S 4 3 において、この予約発信電話番号も比較対象とし、さらに予約発信電話番号と着信時の発信電話番号が一致した場合に限り、第一登録発信電話番号の情報を予約発信電話番号で置き換える。この手順を踏むことにより、以降、何の影響もなくサービスを受けることが可能となる。

【0 0 2 3】また、上述した実施例においては、発信電話番号確認処理をパスワードの確認後に行うものとして

説明した。しかしながら、発信電話番号の確認時に接続拒否となるケースでは、パスワードの入力／確認処理は無意味なものになってしまう。このため、発信電話番号の確認処理は、パスワードの確認前に行う形態としてもよい。

【0 0 2 4】

【発明の効果】以上説明したように、本発明によれば、サービス利用者からの着信の度に発信電話番号通知情報と登録済みの発信電話番号とを照合するようにしたので、より確実なアカウントの確認を行うことができ、第三者によるアカウントの不正利用を防止することができるという利点が得られる。

【図面の簡単な説明】

【図 1】 本発明の実施形態による全体の構成を示すブロック図である。

【図 2】 サービス提供者側のアクセスポイント及びホストコンピュータの詳細な構成が示すブロック図である。

【図 3】 サービス提供者側ホストコンピュータにおける通信サービス開始前の接続確認処理の基本的な動作を示すフローチャートである。

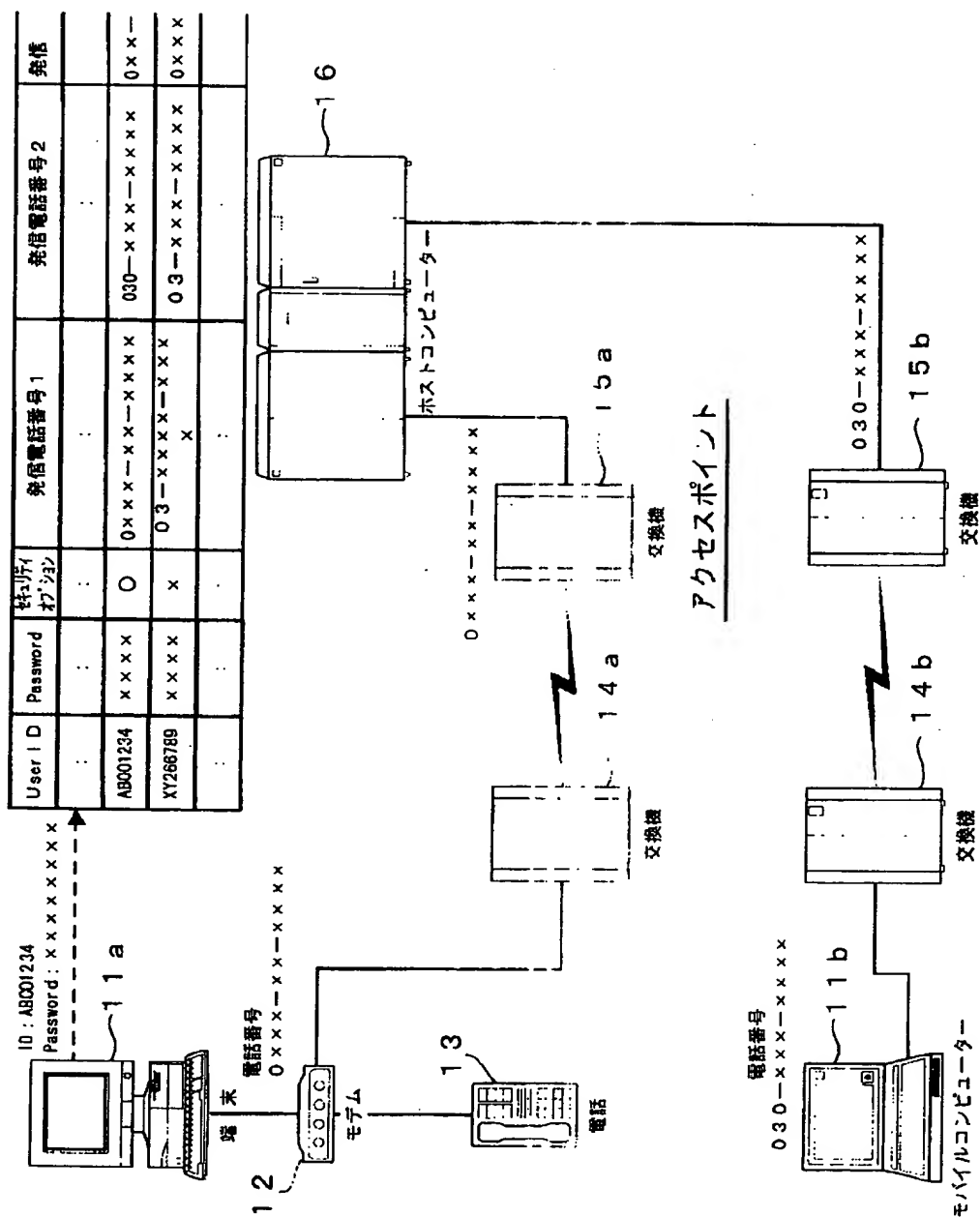
【図 4】 発信電話番号確認処理（ステップ S 3 4）の詳細な動作を説明するためのフローチャートである。

【図 5】 ユーザプロフィール情報 2 6 に定義されている発信電話番号情報を更新する際の処理の動作を説明するためのフローチャートである。

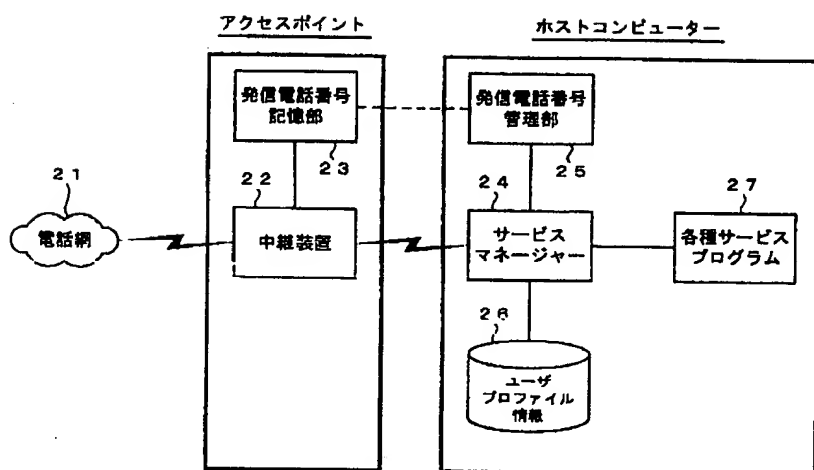
【符号の説明】

- 1 1 a, 1 1 b 端末
- 1 2 モデム
- 1 3 電話
- 1 4 a, 1 5 a, 1 4 b, 1 5 b 交換機
- 1 6 ホストコンピュータ
- 2 1 電話網
- 2 2 中継装置
- 2 3 発信電話番号記憶部
- 2 4 サービスマネージャ
- 2 5 発信電話番号管理部
- 2 6 ユーザプロフィール情報
- 2 7 各種サービスプログラム

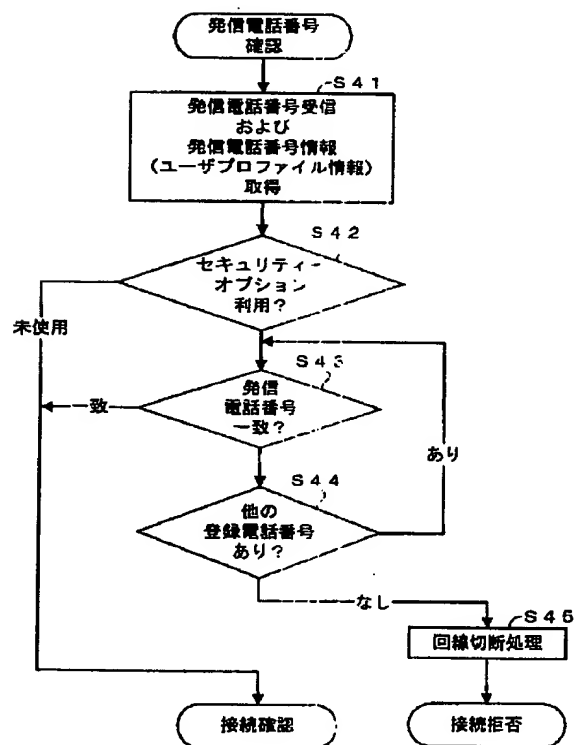
【図 1】



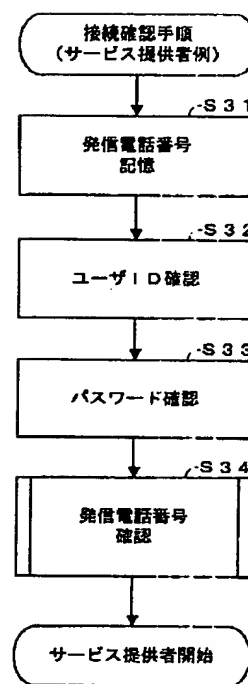
【図 2】



【図 4】



【図 3】



【図 5】

